IFI7045	**Infoturbe haldus**
Maht:	***Kontakttundide maht:*** 20 ***Õppesemester: sügis*** Eksam
Eesmärk:	Anda ülevaade rahvusvaheliselt tunnustatud infoturbemetoodikatest. Luua eeldused teadmiste ja oskuste kujundamiseks infoturbe halduse süsteemi (ITHS) rajamiseks, seireks ja täiustamiseks. Hinnata ITHS kavandamise ja teostamisega seotud organisatsioonilisi vajadusi, eesmärke, turvanõudeid, äriprotsesse ning organisatsiooni suurust ja struktuuri. Oskus hinnata ITHS teostuse mahtu ja ulatust, arvestades organisatsiooni vajadusi ja võimalusi.
Aine lühikirjeldus: ***(sh iseseisva töö sisu kirjeldus vastavuses iseseisva töö mahule)***	Sissejuhatus ainesse: Infoturve ja selle käsitlusala. Infoturbe metoodikad ja standardid ning nende seos teiste IT haldus- ja juhtimisraamistikega (ITIL, Cobit). Kriitilised edutegurid ja infoturbe lähtepunktid. Selgitatakse vajalikud mõisted ja terminid. Teoreetiline osa: Vastavalt ISO 27001/02 ja ISKE standardile käsitletakse järgmiseid teemasid: riskide haldus, infovarade määratlemine, turbeklasside ja -astme määratlemine, turbemeetmete ulatuse ja vajalikkuse hindamine. Infoturbepoliitika koostamine. Jätkusuutlikkuse plaani koostamine. ITHS-i seire ja täiendamine. Praktiline osa: Tundides teostatakse praktilisi ülesandeid, mida on võimalik kasutada arvestustöös.
Õpiväljundid:	Üliõpilane on suuteline hindama organisatsiooni infovarade riske, määratlema turbeastmeid, leidma vajalikud vastumeetmed, koostama infoturbepoliitikaid ja muid regulatsioone. Planeerima ja evitama infoturbe haldussüsteemi, mis baseerub ISO27001/02 või ISKE standardil.
Hindamismeetodid:	Hindeline eksam.
Õppejõud:	Andro Kull
Aine ingliskeelne nimetus:	Information Security Managemenet
Eeldusaine:	Puudub
Kohustuslik kirjandus:	Loengukonspekt
Asenduskirjandus:	http://www.iso27001security.com/
(üliõpilase poolt läbi töötatava kirjanduse loetelu, mis katab	http://www.kriso.ee/Information-Security-Risk-Management-Handbook-Handbook/db/9780580607455.html

ainekursuse loengulist osa)	http://www.ria.ee/iske
Õppetöös osalemise ja eksamile / arvestusele pääsemise nõuded:	Iga üliõpilane osaleb grupitööna valmivas arvestustöös ja selle kaitsmisel seminaris ning sooritab eksami. Eksamile pääsemise eelduseks on arvestustöö esitamine ja kaitsmine. Kõik ühes rühmas osalenud üliõpilased saavad arvestustöö eest sama palju punkte.
Iseseisva töö nõuded:	Iseseisvate tööde loetelu: Arvestustöö rühmatööna: • kaardistatakse ettevõtte infovarad – maksimaalselt 10 punkti; • tehakse riskianalüüs – maksimaalselt 10 punkti; • planeeritakse turvameetmed – maksimaalselt 10 punkti; • koostatakse infoturbe poliitika – maksimaalselt 10 punkti; • koostatakse jätkusuutlikkuse plaan – maksimaalselt 10 punkti. Arvestustöö koostamise juhised antakse loengutes.
Eksami hindamiskriteeriumid või arvestuse sooritamiseks vajalik miinimumtase:	Hindamiskriteeriumid, millest hindamisel lähtutakse: Esitatud ja kaitstud on arvestustöö (maksimaalselt 50 punkti) ning sooritatud on eksam (maksimaalselt 50 punkti), millede summeeritud punktid annavad järgneva hinde: A – 91-100 punkti B - 81-90 punkti C – 71-80 punkti D – 61-70 punkti E – 51-60 punkti
Informatsioon kursuse sisu kohta, kursuse jaotumine teemade kaupa sh kontakttundide ajad:	**I loeng 3.nov. 10-14** Kursuse kirjeldus, ootused kursuse kohta. Sissejuhatus infoturbesse – infoturbe käsitlusala, terminid, mõisted, määratlused: • Mis on info, mida me turvame? • Mis on infoturve? • Olulised mõisted; • Miks on vaja infoturvet? • Infoturbe lähtekohad; • Infoturbe seosed üldise juhtimisega ja IT-juhtimisega; • Juhtkonna kohustused ja vastutused infoturbe alal; • Infoturbe koordineerimine ja delegeerimine; • Infoturve, kui protsess. Riskide kaalutlemine ja analüüs: • Kuidas selgitada välja turbe vajadused? • Turvariskide kaalutlemine; • Infoturbeohud: 1. Füüsilised ohud;

2. Looduslikud ohud;
3. Riistvara ohud;
4. Koostööpartneri ohud;
5. Tarkvara ohud;
6. Küberründed;
7. Inimese põhjustatud ohud.

- Riskide määratlemine ja analüüs;
- Riskide kaalumine ja riskiskaalad;
- Jääkriski määramine ja kinnitamine.

II loeng 17.nov. 10-14

Riskide maandamine:

- Infoturbe standardid ja hea tava;
- Infoturbe halduse protsess.

Infoturbe halduse meetmed:

- Füüsilised infoturbe meetmed;
- Organisatsioonilised infoturbe meetmed;
- Tehnoloogilised infoturbe meetmed.

Infoturbepoliitika:

- Infoturbepoliitika dokument;
- Infoturbe poliitika rakendamine ja kontroll;
- Infoturbepoliitika läbivaatus.

ISO 27001/2 standard:

- Turvapoliitika;
- Infoturbe korraldus;
- Varade haldus;
- Inimressursi turve;
- Füüsiline ja keskkonna turve;
- Side ja käituse haldus;
- Pääsu reguleerimine;
- Infosüsteemide hankimine, väljatöötamine ja hooldus;
- Infoturbeintsidentide haldus;
- Jätkusuutlikkuse haldus;
- Vastavus.

III loeng 1.dets. 10-14

Riskijuhtimine;
Intsidendihaldus:

- Intsidendihalduse ja jätkusuutlikuse plaanimine
- Intsidendi tuvastamine ja kindlaks tegemine
    - Seire (monitooring);
    - Seirelogide kaitse;
    - Tõrgete logimine.
- Intsidendi hindamine;
- Infoturbeintsidendist või -nõrkusest teavitamine

    - Kommunikatsioon ja raporteerimine.
- Intsidendi tagajärgede leevendamine;
- Intsidendi taastamine.

Jätkusuutlikkuse tagamine:

- Talitluspidevuse protsess;
- Talitluspidevuse planeerimine;
- Taaste planeerimine;
- Talitluspidevuse testimine.

Turbenõuete vastavus:

- Vastavus õigusaktide nõuetele;
- Vastavus infoturbepoliitikale;
- Infosüsteemide auditeerimisvajadus;
- Infoturbe dokumentide auditeerimine;
- Infoturbe korralduse auditeerimine.

Infoturbe järelevalve ja auditeerimine.

IV loeng 14.dets. 10-14

Etalonturbe olemus ja astmeline etalonturve;
ISKE määrus ja rakendusjuhend;
ISKE rakendamise 11 sammu:

- Infovarade inventuur ja spetsifitseerimine
- Andmekogude turvaklasside määramine
- Muude infovarade turvaklasside määramine
- Turvaklassiga infovarade turbeastme määramine
- Tsoonide vajaduse analüüs, asutuse tsoneerimine vajadusel
- Tüüpmoodulite märkimine infovarade spetsifikatsioonidesse
- Turbehalduse meetmete loetelu koostamine
- Turvameetmete rakendamise plaani koostamine
- Turvameetmete rakendamine
- Tegeliku turvaolukorra kontroll, ohtude hindamine, vajadusel täiendavate meetmete rakendamine
- Muudatuste haldus (alates 6 versioonist)

ISKE auditeerimine.

V seminar 15.dets. 10-14

Arvestustööde ettekandmine ja kaitsmine.

Täpsemad arvestustöö nõuded ja seminari kirjeldus antakse loengute käigus!